Conference on Disarmament

27 July 2015

Original: English

Australia

Working paper

Protection of sensitive information under FMCT verification[1]

Key points

- Provisions in model IAEA safeguards agreements are likely to provide an appropriate prototype for provisions in an FMCT whose purpose is to avoid or minimise the disclosure of proliferation-related or other sensitive information during verification at civil fuel-cycle facilities.
- Verification of the destruction or conversion of former weapons production facilities, or of the disposition of fuel for naval propulsion may need to be conducted under special managed access frameworks. The managed access provisions in INFCIRC/540 offer suitable principles, but details would need to be developed. Setting in a treaty verification objectives that embody an acceptable compromise between intrusive verification and protection of proliferation-sensitive information may be considered.
- Provisions on FMCT verification at undeclared locations, for example as part of a challenge inspection, may need to be closer to those for such inspections under the Chemical Weapons Convention (CWC) or Comprehensive Nuclear-Test-Ban Treaty (CTBT). Special guidance or technical measures could be considered to address concerns by States to protect particular kinds of sensitive information.
- Provisions on managed access in INFCIRC/540, the CTBT and the CWC (among other instruments) address an important balance between the rights of an inspected state party to protect sensitive information and its obligations to demonstrate

[1] Prepared by Mr. Peter Woolcott, Ambassador of Australia to the Conference on Disarmament (15 February 2010 – 1 September 2014) and Mr. Malcolm Coxhead, Director, Australian Safeguards and Non-Proliferation Office, Nuclear Non-Proliferation Section, Department of Foreign Affairs and Trade.

GE.15-12639 (E)

1512639

Please recycle

Analysis

1. Sensitivity may be attached to information or data related to verification activities because of the risk that unauthorised disclosure could pose for national, commercial interests or for nuclear proliferation. For example, in the case of excess weapon materials, concern over potential access to nuclear-weapon design (e.g. isotopics, classified shapes etc.) will attract strong national security sensitivities. Similarly, enrichment technologies may attract both national security and commercial sensitivities. Information associated with the physical security of nuclear material or facilities (to mitigate against the risk of theft and/or sabotage) will also attract national security sensitivities.

2. Effective procedures to avoid or minimise the disclosure of sensitive information or data during, or obtained from, verification activities is central to the cooperation of states with those activities, and to avoiding damage to the reputation of the verification organisation. Such procedures have been elaborated with respect to International Atomic Energy Agency (IAEA) safeguards, as well as verification under the CWC and CTBT. Minimising disclosure has two broad aspects:

(a) Negotiation of access by (by inspectors or the verification organisation) with the inspected state, the aim of which is to meet verification objectives but avoid the disclosure of sensitive information or data if the disclosure is not needed – often referred to as managed access

(b) Managing the circulation within, protection of, and disclosure beyond the verification organisation of verification information, i.e. need-to-know and confidentiality protections.

3. The model IAEA safeguards agreements INFCIRC/66/Rev.2 (facility–specific safeguards), INFCIRC/153(Corrected) (Comprehensive Safeguards Agreement) and INFCIRC/540 (Corrected) (the Additional Protocol) include provisions on some or all of these elements, as do the CWC and CTBT. Implementation of managed access provisions is done through negotiation with the inspected state, either ahead of time by the verification organisation or, if necessary, on site by inspectors. Implementation of the other measures is done through confidentiality policies and procedures of each of the organisations (those for the CTBT are under development).

Managed Access

4. The following elements on management of access are included in model IAEA safeguards agreements:

(a) INFCIRC/153 (model Comprehensive Safeguards Agreement):

- Does not include a managed access mechanism, but inspector access during routine inspections of nuclear inventory is limited to strategic points[2]
- Requires the Agency to arrange the visits and activities of inspectors to "... ensure protection of industrial secrets or any other confidential information coming to the inspectors" knowledge.

[2] The strategic points do not limit the IAEA's access for design information verification activities. Inspector access during special inspections is arranged "in agreement with the state" (the Board of Governors may press the state to provide additional access).

(b) INFCIRC/66 type agreements provide similarly, although access (whether for routine or special inspection) is defined in terms of access to a facility subject to the agreement.

(c) INFCIRC/540 (model AP):

- Includes a managed access mechanism stating that "Such arrangements shall not preclude the Agency from conducting activities necessary to provide credible assurance of the absence of undeclared nuclear material and activities at the location in question ..."

Verification at civil fuel cycle facilities and with respect to other declared civil activities

5. FMCT verification at civil fuel cycle facilities should be sufficiently similar to IAEA safeguards for the same information and data protection provisions to apply with respect to such facilities. This relates both to controls on access and on protection of confidential information and would be consistent with the aim of negotiating an FMCT that is non-discriminatory. If FMCT verification requires routine verification beyond strategic points, managed access provisions might be extended to such verification.

Managed access for verification at former weapons material production facilities and on the disposition of fuel for military propulsion

6. FMCT verification of the destruction or conversion of former weapons production facilities or on the disposition of fuel for military propulsion would likely need to be conducted under a managed access framework. The managed access provisions in INFCIRC/540 may offer suitable principles, including, importantly, the qualifier that such restrictions not preclude the verification agency from conducting activities necessary to provide credible assurance. It should, in principle, be possible for the verification organisation and the inspected state to negotiate detailed access procedures in advance of routine inspections. However treaty negotiators may wish also to include guidance on the scope and objectives of verification in these cases. Provisions of this kind have been included in bilateral agreements such as the 1997 *Agreement between the Government of The United States of America and the Government of the Russian Federation Concerning Cooperation Regarding Plutonium Production Reactors*. In order to achieve the objectives of the Agreement, the Parties undertake to permit monitoring of specified reactors to ensure that once shut down they remain in a non-operating status, as well as monitoring of other reactors to ensure that they operate only in an agreed mode. Monitoring of certain plutonium is included to ensure it is not used in nuclear weapons. The types of techniques to be applied to effect the monitoring are specified and rely on principles of containment and surveillance. For plutonium monitoring, restricted measurement of radioisotopes provided for.

Managed access for verification at undeclared locations

7. Provisions on FMCT verification at undeclared locations, for example as part of a challenge inspection, may need to be closer to those for such inspections under the CWC or the CTBT. Access under an FMCT challenge inspection could, in principle, involve the most sensitive facilities. Moreover, the opportunity to work out mutually-acceptable and site-specific access procedures in advance of an inspection will not be possible. The CWC and CTBT provisions are similar in most respects. The latter (with which the author is more intimately familiar) provides in relation to managed access, inter alia:

- The inspected State Party has the obligation to provide access within the inspection area for the sole purpose of determining facts relevant to the purpose of the inspection
- The inspected State Party has the right throughout the inspection area to take measures to protect sensitive installations and locations and to prevent disclosure of confidential information not related to the purpose of the inspection
- The inspected State Party has the right to make the final decision regarding any access of the inspection team, taking into account its obligations under this Treaty and the provisions on managed access.
- If the inspected State Party ... restricts access within the inspection area, it shall make every reasonable effort in consultations with the inspection team to demonstrate through alternative means its compliance with this Treaty.

8. The balance captured by these provisions is important for ensuring that the negotiation of managed access arrangements serves the objectives of both the inspected state and the verification organisation. The CTBT provides that the reports of inspections will include an account of cooperation granted by the inspected state, giving an opportunity for the future CTBT Organization's Executive Council an opportunity to review the balance achieved in negotiation of managed access.

Managed access for fissile material in classified forms

9. Managed access concepts for protection of fissile material in classified forms have also been developed by a working group under the so-called "Trilateral Initiative", focusing on IAEA verification of weapon-origin fissile material in the Russian Federation and the United States. An outcome from the initiative was the development of an attribute verification technique for placing classified weapon-origin plutonium under IAEA verification without revealing proliferation sensitive information. In order to confirm that the declared material was authentic, the technique performed attribute verification measurements (whereby an object is compared to a set of reference characteristics) behind information barrier technology to prevent classified information from being transmitted or otherwise conveyed beyond a secure environment. Outcomes from the Trilateral Initiative could facilitate steps by a nuclear weapons possessor state to commit fissile weapons components to verification to ensure they are not returned to weapons use, but did not include lessons for verification of the conversion of fissile components to unclassified forms and thus quantitative incorporation as stocks under an FMCT.

10. The so called UK-Norway initiative has also examined a number of the key challenges for protection of sensitive information during verification of the dismantlement of nuclear warheads. The sensitivities considered have not been limited to proliferation sensitivity, but also national and nuclear security concerns. So far work has been targeted at particular practical challenges. Concepts immediately useful for inclusion in treaty-level guidance in an FMCT have not been a focus of the work. The concepts and techniques developed in relation to information barriers, data and equipment authentication, and containment and surveillance tools may nevertheless offer specific lessons useful for an FMCT.

Confidentiality procedures

11. The following elements on protection of confidential information are included in model IAEA safeguards agreements. These provisions provide a good model for much of the verification likely to be required under an FMCT.

(a) INFCIRC/153 (model CSA):

- requires the Agency to "take every precaution to protect commercial and industrial secrets and other confidential information coming to its knowledge in the implementation of the Agreement"
- requires that communication of information relating to safeguards implementation "may be given to the Board of Governors and to such Agency staff members as require such knowledge by reason of their official duties in connection with safeguards, but only to the extent necessary for the Agency to fulfil its responsibilities in implementing the Agreement."

(b) INFCIRC/540 (model AP):

- Article 15 provides that

  (a) The Agency shall maintain a stringent regime to ensure effective protection against disclosure of commercial, technological and industrial secrets and other confidential information coming to its knowledge, including such information coming to the Agency's knowledge in the implementation of this Protocol.

  (b) The regime referred to in paragraph a. above shall include, among others, provisions relating to:

  (i) General principles and associated measures for the handling of confidential information;

  (ii) Conditions of staff employment relating to the protection of confidential information;

  (iii) Procedures in cases of breaches or alleged breaches of confidentiality.

  (c) The regime referred to in paragraph a. above shall be approved and periodically reviewed by the Board.

12. The CWC, in its Annex on Confidentiality, goes into greater detail than other treaties on measures for the protection of confidential information gathered during verification activities. It requires the Director-General to establish a stringent regime governing the handling of confidential information by the Technical Secretariat, and provides guidance on the classification of information based on its level of sensitivity. It also details the circumstances in which verification data could be released. This includes data provided to States Parties to help assure them of the continued compliance of other States Parties. The CWC's confidentiality regime has been described as overly stringent. Its strongest provisions may be appropriate for the most sensitive information. However the explicit role of states in classifying data makes over-classification a risk.

Additional measures

13. Additional technical measures have been developed for the CWC and CTBT to address concerns by States to protect particular kinds of sensitive information. Procedures have been developed (inter-alia):

- for checking of inspection equipment by the inspected state
- for escorting of inspectors
- for sample taking and analysis
- for decontamination of clothing and equipment surfaces (or the use of disposable items), to prevent the disclosure of sensitive data if these are taken off-site
- to purge computer equipment of data
- to manage photography so that non-relevant information is not included
- to hold more sensitive information on-site under joint seal, either during or after an inspection.

14. Detailed guidance on the application of these sorts of measures is being addressed for the CTBT in the Operational Manual for On-Site Inspection (OSI) that is being negotiated by States Signatories, as well as in policies being developed by the CTBTO's Provisional Technical Secretariat. A similar manual for challenge inspections under the CWC has been developed under the control of the OPCW's Technical Secretariat. The development of these arrangements is not based purely on theoretical considerations. Both the CWC and CTBTO carry out inspection exercises that put procedures to the test. In November-December of 2014 the CTBTO will conduct a major OSI exercise over several weeks in Jordan. Lessons from that work should help to refine OSI procedures.

15. As discussions among states on the draft OSI Operational Manual for the CTBT have proceeded, a number of lessons for future treaty drafters have emerged. Key amongst these is the importance of ensuring that various treaty provisions and terminology are clear and can work effectively together.

16. Probably the hardest risk to address in relation to the protection of sensitive information is the inspector. There are no (permitted) techniques to purge information from inspector memory. Disciplinary or legal action can deter unauthorised disclosure, but is not an easy solution. In so far as there may be a concern about the reliability of individual inspectors, INFCIRC/153, INFCIRC/540, the CWC and CTBT offer scope for states to reject the designation of particular persons for inspection in their territory. Other requirements, such as for another inspector to be present when sensitive information is accessed, are possible also. The negotiation of effective managed access arrangements is the best solution however, in order to avoid exposing inspectors to sensitive information.